

## A B S T R A C T

The invention relates to a method of managing alerts  
5 issued by intrusion detection sensors (11a, 11b, 11c) of  
an information security system (1) including an alert  
management system (13), each alert being defined by an  
alert identifier and an alert content, the method  
including the following steps:

10       · associating with each of the alerts issued by the  
intrusion detection sensors (11a, 11b, 11c) a description  
including a conjunction of valued attributes belonging to  
attribute domains;

15       · organizing the valued attributes belonging to each  
attribute domain into a taxonomic structure defining  
generalization relationships between said valued  
attributes, the plurality of attribute domains thus  
forming a plurality of taxonomic structures;

20       · completing the description of each of said alerts  
with sets of values induced by the taxonomic structures  
on the basis of the valued attributes of said alerts to  
form complete alerts; and

25       · storing said complete alerts in a logic file  
system (21) to enable them to be consulted.

25

30

Translation of the title and the abstract as they were when originally filed by the  
Applicant. No account has been taken of any changes that may have been made  
subsequently by the PCT Authorities acting ex officio, e.g. under PCT Rules 37.2,  
35 38.2, and/or 48.3.